AMENDMENTS TO THE CLAIMS

This listing of the claims will replace all prior versions and listing of the claims.

Listing of the Claims:

1. (Currently amended) A function randomness evaluating apparatus for a data encryption device comprising:

input means for inputting digital signals representing candidate functions S(x) of S-box to be evaluated, input difference value Δx and output mask values Γy, and storing them in storage means;

differential-linear-cryptanalysis resistance evaluating means for: counting, for every ~~all~~ sets of input difference value Δx except 0 and output mask value Γy except 0 of each of the functions S(x) read out of the storage means, a number of inputs values x for which the inner product of (S(x)+S(x+Δx)) and said output mask value Γy is 1, as expressed by the following equation:

$$\xi_S(\Delta x, \Gamma y) = \left| 2 \times \#\{x \in GF(2)^n \,|\, (S(x) + S(x+\Delta x)) \bullet \Gamma y = 1\} - 2^n \right|;$$

determining a maximum value Ξ among the results of counting;

evaluating the resistance of said function to said differential-linear cryptanalysis based on said maximum value Ξ; and

output means for outputting an output digital signal representing an evaluation result.

~~and evaluating the resistance of said function to differential-linear cryptanalysis based on the result of said number; and~~

~~output means for outputting an output digital signal representing an evaluation result.~~

2. Canceled

3. (Currently amended) The function randomness evaluating apparatus of claim 1 ~~or 2~~, further comprising at least one of:

differential-cryptanalysis resistance evaluating means for calculating, for the function S(x) to be evaluated, the number of input values x that satisfy $S(x)+ S(x+\Delta x)=\Delta y$ for every set $(\Delta x, \Delta y)$ and evaluating the resistance of said function to differential cryptanalysis based on the result of said calculation; and

linear-cryptanalysis resistance evaluating means for calculating, for the function to be evaluated, the number of input values x for which the inner product of the input value x and its mask value Γx is equal to the inner product of a function output value S(x) and its mask value Γy and evaluating the resistance of said function to linear cryptanalysis based on the result of said calculation.

4. Canceled

5. Canceled

6. (Previously presented) A random function generating apparatus for a data encryption device comprising:

input means for inputting digital signals representing parameter values of each of a plurality of functions of different algeraic structures and storing them in storage means;

candidate function generating means for generating candidate functions each formed by a combination of said plurality of functions of different algebraic structures based on said plurality of parameters read out of the storage means;

resistance evaluating means for evaluating the resistance of each of said candidate functions to a cryptanalysis; and

selecting means for selecting those of said resistance-evaluated candidate functions which are highly resistant to said cryptanalysis and outputting digital signals representing selected ones of said resistance-evaluated candidate functions;

wherein one of said plurality of functions of different algebraic structures is resistant to each of differential cryptanalysis and linear cryptanalysis.

7. Canceled

8. (Previously presented) The random function generating apparatus of claim 6, wherein said input means is adapted to input digital signals representing input difference values Δx and output mask values Γy and storing them in the storage means, and said resistance evaluating means comprises at least one of:

higher-order-differential cryptanalysis resistance evaluating means for: calculating a minimum value of the degree of a Boolean polynomial for input bits by which output bits of each of said candidate functions are expressed; and evaluating the resistance of said each candidate function to higher order cryptanalysis based on the result of said calculation;

interpolation-cryptanalysis resistance evaluating means for: expressing an output value y as $y = f_k(x)$ for an input value x and a fixed key k using a polynomial over Galois field which is composed of elements equal to a prime p or a power of said prime p; counting a number of terms

of said polynomial; and evaluating the resistance of said each candidate function to interpolation cryptanalysis based on the result of said number;

partitioning-cryptanalysis resistance evaluating means for: dividing all input values of the function to be evaluated and the corresponding output values into input subsets and output subsets; calculating an imbalance of the relationships between the input subset and the output subset with respect to their average corresponding relationship; and evaluating the resistance of said function to partitioning cryptanalysis based on the result of said calculation; and

differential-linear cryptanalysis resistance evaluating means for: calculating, for every set of input difference value Δx and output mask value Γy of the function $S(x)$ to be evaluated, a number of input values x for which the inner product of $(S(x)+S(x+\Delta x))$ and said output mask value Γy is 1; and evaluating the resistance of said function to differential-linear cryptanalysis based on the result of said calculation.

9. (Currently amended) A method for evaluating the randomness of the input/output relationship of a function for data encryption, said method comprising:

inputting digital signals representing candidate functions $S(x)$ of S-box to be evaluated, input difference values Δx and output mask values Γy, and storing them in storage means;

a differential-linear cryptanalysis resistance evaluating step of: counting, for every set of input difference value Δx <u>except 0</u> and output mask value Γy <u>except 0</u> of each of the functions $S(x)$ read out of the storage means, a number of input values x for which an inner product of $(S(x)+S(x+\Delta x))$ and said output mask value Γy is 1<u>, as expressed by the following equation:</u>

$$\underline{\xi_S(\Delta x, \Gamma y) = \left|2 \times \#\{x \in GF(2)^n \middle| (S(x) + S(x+\Delta x) \bullet \Gamma y = 1\} - 2^n\right|;}$$

<u>determining a maximum value Ξ among the results of counting;</u>

evaluating the resistance of said function to said differential-linear cryptanalysis using said maximum value Ξ; and

outputting an output digital signal representing an evaluation result.

~~; and evaluating resistance of said function to differential-linear cryptanalysis based on the result of said number; and~~

~~outputting an output digital signal representing an evaluation result.~~

10. Canceled

11. (Currently amended) The randomness evaluating method of any one of claim 9, ~~10,~~ 35 or 36, further comprising at least one of:

(d) a differential-cryptanalysis resistance evaluating step of: calculating the number of input values x that satisfy S(x)+ S(x+Δx)=Δy for every set (Δx, Δy) except Δx=0; and evaluating the resistance of said function to differential cryptanalysis based on the result of said calculation; and

(e) a linear-cryptanalysis resistance evaluating means for calculating, for said function S(x), the number of input values x for which the inner product of the input value x and its mask value Γx is equal to the inner product of a function output value S(x) and its mask value Γy and evaluating the resistance of said function to linear cryptanalysis based on the result of said calculation.

12. Canceled

13. (Currently amended) A random function generating method for data encryption comprising the steps of:

(o) inputting digital signals representing input difference values Δx, output mask values Γy and parameter values of each of a plurality of functions of different algebraic structures and storing them in storage means;

(a) setting various input values read out of the storage means for each of candidate functions $S(x)$ of S-box and calculating output values corresponding to said various input values x;

(b) storing the output values in storage means; and

(c) evaluating the resistance of each of said candidate functions to a cryptanalysis based on the output values stored in said storage means, and selectively outputting candidate function highly resistant to said cryptanalysis; and

wherein said step (c) comprising:

(c-1) a higher-order cryptanalysis resistance evaluating step of: calculating a minimum value of the degree of a Boolean polynomial for input bits of each of said candidate functions by which its output bits are expressed; evaluating the resistance of said each candidate function to higher order cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined first reference and discarding the others;

(c-2) a differential-linear cryptanalysis resistance evaluating step of: calculating, for every set of input difference value Δx and output mask value Γy of each candidate function $S(x)$, a number of input values x for which the inner product of $(S(x)+S(x+\Delta x))$ and said output mask value Γy is 1; evaluating resistance of said function to differential-linear cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined second reference and discarding the others;

(c-3) a partitioning-cryptanalysis resistance evaluating step of: dividing all input values of each candidate function and the corresponding output values into input subsets and output subsets; calculating an imbalance of the relationship between the input subset and the output subset with respect to their average corresponding relationship; evaluating the resistance of said each candidate function to said partitioning cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined third reference and discarding the others; and

(c-4) an interpolation-cryptanalysis resistance evaluating step of: expressing an output value y as $y = f_k(x)$ for an input value x and a fixed key k using a polynomial over Galois field which is composed of elements equal to a prime p or a power of said prime p; counting a number of terms of said polynomial; evaluating the resistance of said function to interpolation cryptanalysis; and leaving those of said candidate functions whose resistance is higher than a predetermined fourth reference and discarding the others;

<u>wherein said candidate functions are each a composite function composed of at least one function resistant to said differential cryptanalysis and said linear cryptanalysis and at least one function of an algebraic structure different from that of said at least one function</u>.

14. (Previously presented) The random function generating method of claim 13, wherein:

said differential-linear-cryptanalysis resistance evaluating step (c-2) includes a step of: calculating the following equation for every set of said input difference value Δx except 0 and said output mask value Γy except 0

$$\xi_S(\Delta x, \Gamma y) = \left| 2 \times \# \{ x \in GF(2)^n \middle| (S(x) + S(x + \Delta x)) \bullet \Gamma y = 1 \} - 2^n \right|;$$

calculating a maximum value Ξ among the calculation results; and evaluating the resistance of said candidate function to said differential-linear cryptanalysis based on said maximum value Ξ; and

said partitioning cryptanalysis resistance evaluating step (3) includes a step of dividing an input value set F and an output value set G of said function into u input subsets $\{F_0, F_1, \ldots, F_{u-1}\}$ and v output subsets $\{G_0, G_1, \ldots, G_{v-1}\}$; for each partition-pair (F_i, G_j) ($i = 0, \ldots, u-1$; $j = 0, 1, \ldots, v-1$), calculating a maximum one of probabilities that all output values y corresponding to all input values x of the input subset F_i belong to the respective output subsets G_j ($j = 0, \ldots, v-1$); calculating a measure $I_S(F, G)$ of an average imbalance of a partition-pair (F, G) based on all maximum values calculated for all partition pairs; and evaluating the resistance of said candidate function to said partitioning cryptanalysis based on said measure.

15. (Original) The random function generating method of claim 13 or 14, wherein:

said step (c-1) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said first reference by a first predetermined width, and executing again the evaluation and selecting process;

said step (c-2) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said second reference by a second predetermined width, and executing again the evaluation and selecting process;

said step (c-3) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said third reference by a third predetermined width, and executing again the evaluation and selecting process; and

said step (c-4) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said fourth reference by a fourth predetermined width, and executing again the evaluation and selecting process.

16. (Previously presented) The random function generating method of claim 13 or 14, further comprising:

(c-5) a differential-cryptanalysis resistance evaluating step of: calculating, for each candidate function S(x), the number of inputs x that satisfy $S(x)+S(x+\Delta x)=\Delta y$ for every set $(\Delta x, \Delta y)$ except $\Delta x=0$; evaluating the resistance of said each candidate function to differential cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined fifth reference and discarding the others before said step (c-2); and

(c-6) a linear-cryptanalysis resistance evaluating step of: calculating, for each candidate function, the number of input values x for which the inner product of the input value x and its mask value Γx is equal to the inner product of a function output value S(x) and its mask value Γy; evaluating the resistance of said each candidate function to linear cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined sixth reference and discarding the others after said step (c-5).

17. Canceled

18. (Previously presented) The random function generating method of claim 16, wherein:

said step (c-5) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said fifth reference by a fifth predetermined width, and executing again the evaluation and selecting process; and

said step (c-6) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said sixth reference by a sixth predetermined width, and executing again the evaluation and selecting process.

19. Canceled

20. (Currently amended) A recording medium having recorded thereon a random function generating method for data encryption as a computer program, said program comprising the steps of:

(a) setting various values as each parameter for candidate functions S(x) and calculating output values corresponding to various input values;

(b) storing the output values in storage means; and

(c) evaluating resistance of each of said candidate functions to a cryptanalysis based on the output values stored in said storage means, and selectively outputting candidate function highly resistant to said cryptanalysis; and

wherein said step (c) comprises:

(c-1) a higher-order cryptanalysis resistance evaluating step of: calculating a minimum value of the degree of a Boolean polynomial for input bits of each of said candidate functions by which its output bits are expressed; evaluating the resistance of said each candidate function to higher order cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined first reference and discarding the others;

(c-2) a differential-linear cryptanalysis resistance evaluating step of: calculating, for every set of input difference value Δx and output mask value Γy of each candidate function $S(x)$, a number of input values x for which the inner product of $(S(x)+S(x+\Delta x))$ and said output mask value Γy is 1; evaluating resistance of said function to differential-linear cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined second reference and discarding the others;

(c-3) a partitioning-cryptanalysis resistance evaluating step of: dividing all input values of each candidate function and the corresponding output values into input subsets and output subsets; calculating an imbalance of the relationship between the input subset and the output subset with respect to their average corresponding relationship; evaluating the resistance of said each candidate function to said partitioning cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined third reference and discarding the others; and

(c-4) an interpolation-cryptanalysis resistance evaluating step of: expressing an output value y as $y = f_k(x)$ for an input value x and a fixed key k using a polynomial over Galois field which is composed of elements equal to a prime p or a power of said prime p; counting a number of terms of said polynomial; evaluating the resistance of said function to interpolation cryptanalysis; and leaving those of said candidate functions whose resistance is higher than a predetermined fourth reference and discarding the others;

wherein said candidate functions are each a composite function composed of at least one function resistant to said differential cryptanalysis and said linear cryptanalysis and at least one function of an algebraic structure different from that of said at least one function.

21. (Previously presented) The recording medium of claim 20, wherein:

said differential-linear-cryptanalysis resistance evaluating step (c-2) includes a step of: calculating the following equation for every set of said input difference Δx except 0 and said output mask value Γy except 0

$$\xi_S(\Delta x, \Gamma y) = \left| 2 \times \# \{ x \in GF(2)^n \middle| (S(x) + S(x + \Delta x)) \bullet \Gamma y = 1 \} - 2^n \right|;$$

calculating a maximum value Ξ among the calculation results; and evaluating the resistance of said candidate function to said differential-linear cryptanalysis based on said maximum value Ξ; and

said partitioning cryptanalysis resistance evaluating step (3) includes a step of dividing an input value set F and an output value set G of said function into u input subsets $\{F_0, F_1, \ldots, F_{u-1}\}$ and v output subsets $\{G_0, G_1, \ldots, G_{v-1}\}$; for each partition-pair (F_i, G_j) $(i = 0, \ldots, u-1; j = 0, 1, \ldots, v-1)$, calculating a maximum one of probabilities that all output values y corresponding to all input values x of the input subset F_i belong to the respective output subsets G_j $(j = 0, \ldots, v-1)$; calculating a measure $I_S(F, G)$ of an average imbalance of a partition-pair (F, G) based on all maximum values calculated for all partition pairs; and evaluating the resistance of said candidate function to said partitioning cryptanalysis based on said measure.

22. (Original) The recording medium of claim 20 or 21, wherein:

said step (c-1) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said first reference by a first predetermined width, and executing again the evaluation and selecting process;

said step (c-2) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said second reference by a second predetermined width, and executing again the evaluation and selecting process;

said step (c-3) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said third reference by a third predetermined width, and executing again the evaluation and selecting process; and

said step (c-4) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said fourth reference by a fourth predetermined width, and executing again the evaluation and selecting process.

23. (Previously presented) The recording medium of claim 20 or 21, wherein said program includesat least one of:

(c-5) a differential-cryptanalysis resistance evaluating step of: calculating, for each candidate function S(x), the number of inputs x that satisfy S(x)+ S(x+Δx)=Δy for every set (Δx, Δy) except Δx=0; evaluating the resistance of said each candidate function to differential cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined fifth reference and discarding the others before said step (c-2); and

(c-6) a linear-cryptanalysis resistance evaluating step of: calculating, for each candidate function, the number of input values x for which the inner product of the input value x and its mask value Γx is equal to the inner product of a function output value S(x) and its mask value Γy; evaluating the resistance of said each candidate function to linear cryptanalysis based on the result of said calculation; and leaving those of said candidate functions whose resistance is higher than a predetermined sixth reference and discarding the others after step (c-5).

24. Canceled

25. (Previously presented) The recording medium of claim 23, wherein:

said step (c-5) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said fifth reference by a fifth predetermined width, and executing again the evaluation and selecting process; and

said step (c-6) includes a step of: when no candidate function remains undiscarded, easing the candidate function selecting condition by changing said sixth reference by a sixth predetermined width, and executing again the evaluation and selecting process.

26. Canceled

27. (Currently amended) A recording medium having recorded thereon as a program a method for evaluating the randomness of the input/output relationship of a function for data encryption, said program comprising:

(a) a differential-linear cryptanalysis resistance evaluating step of: calculating, for every set of input difference value Δx except 0 and output mask value Γy except 0 of a function S(x) to be evaluated, a number of input values x for which the inner product of (S(x)+S(x+Δx)) and said output mask value Γy is 1, as expressed by the following equation:

$$\xi_S(\Delta x, \Gamma y) = \left| 2 \times \# \{x \in GF(2)^n \middle| (S(x) + S(x+\Delta x) \bullet \Gamma y = 1\} - 2^n \right|;$$

determining a maximum value Ξ among the results of counting;

evaluating the resistance of said function to said differential-linear cryptanalysis using said maximum value Ξ; and

outputting an output digital signal representing an evaluation result.

~~; and evaluating resistance of said function to differential linear cryptanalysis based on the result of the said calculation.~~

28. Canceled

29. (Currently amended) The recording medium of claim 27~~-or 28~~, said program further comprising at least one of:

(e) a differential-cryptanalysis resistance evaluating step of: calculating a number of input values x that satisfy $S(x)+ S(x+\Delta x)=\Delta y$ for every set $(\Delta x, \Delta y)$ except $\Delta x=0$; and evaluating the resistance of said function to differential cryptanalysis based on the result of said calculation; and

(f) a linear-cryptanalysis resistance evaluating means for calculating, for said function S(x), the number of input values x for which the inner product of the input value x and its mask value Γx is equal to the inner product of a function output value S(x) and its mask value Γy and evaluating the resistance of said function to linear cryptanalysis based on the result of said calculation.

30. Canceled

31. (Previously presented) The random function generating method of claim 15, wherein said candidate functions are each a composite function composed of at least one function resistant to said differential cryptanalysis and said linear cryptanalysis and at least one function of an algebraic structure different from that of said at least one function.

32. (Previously presented) The recording medium of 22, wherein said candidate functions are each a composite function composed of at least one function resistant to said differential cryptanalysis and said linear cryptanalysis and at least one function of an algebraic structure different from that of said at least one function.

33. (Currently amended) The function randomness evaluating apparatus of claim 1 ~~or 2~~, further comprising at least one of:

higher-order-differential cryptanalysis resistance evaluating means for calculating a minimum value of the degree of a Boolean polynomial for input bits by which output bits of the function to be evaluated are expressed, and evaluating that larger said minimum value, higher the resistance of said function to higher order differential cryptanalysis is;

interpolation-cryptanalysis resistance evaluating means for: expressing an output value y as $y = f_k(x)$ for an input value x and a fixed key k using a polynomial over Galois field which is composed of elements equal to a prime p or a power of said prime p; counting a number of terms of said polynomial; and evaluating the resistance of said function to interpolation cryptanalysis based on the result of said number; and

partitioning-cryptanalysis resistance evaluating means for: dividing all inputs values of the function to be evaluated and the corresponding output values into input subsets and output subsets; calculating an imbalance of the relationship between the input subset and the output subset with respect to their average corresponding relationship; and evaluating the resistance of said function to partitioning cryptanalysis based on the result of said calculation.

34. (Previously presented) The function randomness evaluating apparatus of claim 33, wherein:

said partitioning-cryptanalysis resistance evaluating means is means for: dividing an input value set F and an output value set G of said function into u input subsets $\{F_0, F_1, \ldots, F_{Fu-1}\}$ and v output subsets $\{G_0, G_1, \ldots, G_{v-1}\}$; for each partition-pair (F_i, G_i) ($i = 0, \ldots, u-1; j = 0, 1, \ldots, v-1$), calculating a maximum one of probabilities that all output value y corresponding to all input values x of the input subset F_i belong to the respective output subsets G_j ($j = 0, \ldots, v-1$); calculating a measure $I_S(F, G)$ of an average imbalance of a partition-pair (F, G) based on all maximum values calculated for all partition pairs; and evaluating the resistance of said function to said partitioning cryptanalysis based on said measure.

35. (Currently amended) The randomness evaluating method of claim ~~9 or 10~~, further comprising at least one of:

(a) a higher-order-differential cryptanalysis resistance evaluating step of: calculating a minimum value of the degree of a Boolean polynomial for input bits of said function S(x) by which its output bits are expressed; and evaluating the resistance of said function to higher order cryptanalysis based on the result of said calculation;

(b) a partitioning-cryptanalysis resistance evaluating step of: dividing all input values of the function to be evaluated and the corresponding output values into input subsets and output subsets; calculating an imbalance of the relationship between the input subset and the output subset with respect to their average corresponding relationships; and evaluating the resistance of said function to partitioning cryptanalysis based on the result of said calculation; and

(c) an interpolation-cryptanalysis resistance evaluating step of: expressing an output value y as $y = f_k(x)$ for an input value x and a fixed key k using a polynomial over Galois field which is composed of elements equal to a prime p or a power of said prime p; counting a number

of terms of said polynomial; and evaluating the resistance of said function to interpolation cryptanalysis.

36. (Previously presented) The randomness evaluating method of claim 35, wherein:

said partitioning-cryptanalysis resistance evaluating step (b) is a step of: dividing an input value set F and an output value set G of said function into u input subsets $\{F_0, F_1, \ldots, F_{u-1}\}$ and v output subsets $\{G_0, G_1, \ldots, G_{v-1}\}$; for each partition-pair (F_i, G_j) $(i = 0, \ldots, u-1; j = 0, 1, \ldots, v-1)$, calculating a maximum one of probabilities that all output values y corresponding to all input values x of the input subset F_i belong to the respective output subsets G_j $(j = 0, \ldots, v-1)$; calculating a measure $I_S(F, G)$ of an average imbalance of a partition-pair (F, G) based on all maximum values calculated for all partition pairs; and evaluating the resistance of said function to said partitioning cryptanalysis based on said measure.

37. (Currently amended) The recording medium of claim 27~~-or 28~~, further comprising at least one of:

(b) a higher-order-differential cryptanalysis resistance evaluating step of: calculating a minimum value of the degree of a Boolean polynomial for input bits of said function S(x) by which its output bits are expressed; and evaluating the resistance of said function to higher order cryptanalysis based on the result of said calculation;

(c) a partitioning-cryptanalysis resistance evaluating step of: dividing all input values of the function to be evaluated and the corresponding outputs into input subsets and output subsets; calculating an imbalance of the relationships between the input subset and the output subset with respect to their average corresponding relationship; and evaluating the resistance of said function to partitioning cryptanalysis based on the result of said calculation; and

(d) an interpolation-cryptanalysis resistance evaluating step of: expressing an output value y as $y = f_k(x)$ for an input value x and a fixed key k using a polynomial over Galois field which is composed of elements equal to a prime p or a power of said prime p; counting a number of terms of said polynomial; and evaluating the resistance of said function to interpolation cryptanalysis.

38. (Previously presented) The recording medium of claim 37, wherein:

said partitioning-cryptanalysis resistance evaluating step (c) is a step of: dividing an input value set F and an output value set G of said function into u input subsets $\{F_0, F_1, \ldots, F_{u-1}\}$ and v output subsets $\{G_0, G_1, \ldots, G_{v-1}\}$; for each partition-pair (F_i, G_i) $(i = 0, \ldots, u-1; j = 0, 1, \ldots, v-1)$, calculating a maximum one of probabilities that all output values y corresponding to all input values x of the input subset F_i belong to the respective output subsets G_j $(j = 0, \ldots, v-1)$, calculating a measure $I_S(F, G)$ of an average imbalance of a partition-pair (F, G) based on all maximum values calculated for all partition pairs; and evaluating the resistance of said function to said partitioning cryptanalysis based on said measure.